Security Principles and Practices Questions

**What are the 3 types of assets covered in "assets protection"? People info and property**

**Which group contains only mixed (tangible/intangible) assets? Intellectual property, geographical**

**Location and proprietary processes**

**What term is defined as "the integration of traditional physical security and information systems security functions into one security protocol? Integrtion**

\*\*\* **What are the 5 avenues for addressing risk? Avoidance, Spreading, Reduction, Acceptance**

**The pooling of risks from more than one source is referred to as \_\_\_\_\_. Risk spreading**

The **Five Ds** are a set of security principles that complement the legal approach.  Though not all five elements are always considered, or can be captured in a D-word, the basic logic underpinning the system can be summarized as noted below.

In this system, the first goal in protecting assets is to **deter** attacks. This may be through warning

**What is the first goal in protecting assets? Deter perps**

ISO 9000 (quality management) or ISO 27000 (information security)What kind of standards do ANSI and ISO issue? Voluntary

**Which staff members are typically concerned with specific processes and activities? Front Line**

**Supervisors**

**What is true about security awareness training that is fun for staff? More engaging than other types of**

**Training**

**A new CSO joins an organization with a freewheeling environment where there has never been a formal security function. What type of obstacle to security training would the CSO most likely receive?**

**Organizational Culture**

**metrics**—that is, a standard of measurement using quantitative, statistical, and/or mathematical analysis.

**Which of the following doesn't constitute a security awareness metric? False alarm reductions after**

**the installation of a new alarm system**

**Policies** establish rules, while **procedures** explain how to follow those rules.

**Systematic Incident Reporting**

An incident reporting system does two critical things:

* Provides a history of events impacting the organization.
* Provides a basis for professional efforts at asset recapture or recovery, or incident reduction or termination.

**Which is not typically included in an incident report policy? Requiring immediate submission**

**How do most organizations deal with decentralized, sporadic incident reporting? They ignore the**

**Incidents or expense losses**

**What is the ultimate value of incident reporting? It prevents future incidents**

**Which data-validation method usually generates richer and more in-depth information than the other methods and provides research flexibility? Fieldwork**

A security manager should:

* Conduct operations in the least expensive, cost-effective way.
* Maintain the lowest costs consistent with required operational results.
* Ensure that the money spent generates the highest possible return.

Cost-effectiveness in asset protection requires balancing expenditures against results and revising the plan as needed. It also requires critical judgment based on a complete understanding of the enterprise operations, a broad knowledge of state-of-the-art security, and the recognition that some elements of the security program may take several years to implement.

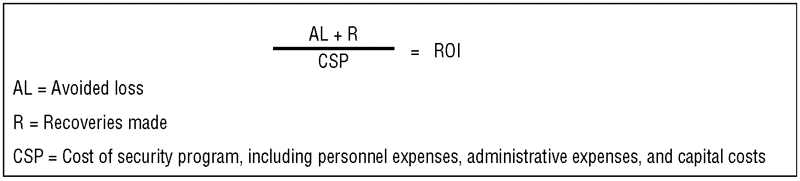
To senior management, what is the primary factor in determining the size or existence of the asset protection program? Cost effectiveness

**What are the least expensive countermeasures an organization can employ? Procedural controls**

**Return on investment** (ROI) is a standard profitability ratio that measures the net income a business earns for each dollar invested. ROI is used to gauge management’s overall effectiveness in generating profits.

ROI can be measured in time saved, improved efficiency, reduced manpower, reduced losses, lower liability or insurance payments, greater customer satisfaction, more secure employees, increased productivity, reduced employee turnover, cost savings, actual revenue, reduced false alarms, saved lives, or anything else that can be quantified. It all translates into an improved bottom line over time.

One way to determine ROI is shown here:



**Which formula for calculating ROI is correct? Avoided loss +recoveries made = cost of security**

**Program**

In the case of nuisance fire alarms, hard costs might be: Lost staff productivity

What term is defined as "the process of measuring an asset protection program’s costs and benefits as well as its successes and failures? Security metrics

Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.An asset protection program is cost-justified if it is established that probable real losses would not occur if the proposed asset protection measures were adopted. In that approach, **cost avoidance** is the total cost of probable security losses prevented. Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.Asset protection programs prevent other losses, including some that are rarely quantified. A good example is the work of security patrols in observing and correcting maintenance or housekeeping problems while at the same time preventing hazards such as fires.The real test would be whether the actual losses were less than the probable losses and whether the combined cost of the actual losses and the cost of maintaining the asset protection organization were within the risk-assumption boundaries accepted by management when approving the asset protection program.

**Definition of Risk**

The *ASIS International General Risk Security Guideline* defines **risk**as the possibility of loss resulting from a threat, security incident, or event.  Put another way:  Risk refers to all the adverse outcomes that an organization wishes to avoid and is a function of the probability that such consequences will occur, their magnitude, and their imminence.

**What term refers to "all the adverse outcomes that an organization wishes to avoid and is a function of the probability that such consequences will occur, their magnitude, and their imminence?" risk**

**Asset Identification**

Asset identification is critical to an estimate of risk at a site. There are several ways to approach this effort, almost all of which assign a value to the asset. This value has been described as **criticality, consequence of loss, or severity**.

Consequence criteria is determined by valuing the damage an entity may suffer.

* Example: Loss of a copier machine may cause employees to go to a different area and lose 15-20 minutes of productive labor time. Loss of an R&D folder could paralyze the entire project, cause damage to reputation, loss of future profits, and other  sunken costs.
* Example: Replacing a copy machine may cost $5,000, but replacing a folder with an entire R&D development portfolio may be worth $100 million.

**Which is not one of the three general methods of valuing assets? Policy**

**Risk Assessment**

Risk assessment examines the outcome of a successful adversary attack, the likelihood it will occur, how it will unfold, and how many people will be affected. In risk assessment, the analyst attempts to answer three questions:

* What can go wrong?
* What is the likelihood that it could go wrong?
* What are the consequences?

**Which type of risk assessment methods examine the why and how of decision making, not just what, where, when, or who? Qualitative**

Inductive reasoning begins with an event (The facility is attacked.) and reasons from data to reach a conclusion as to how best to protect the facility.  Deductive reasoning begins with a  conjecture,"What if the facility is attacked?" and explores possibilities to determine how best to protect the site.

**Which risk assessment technique proceeds from observation to pattern to hypothesis to theory?**

Deductive reasoning- Starts with “What if?” What if the facility is attacked?....

**Risk Management**

Risk management builds on risk assessment by answering a second set of questions:

* What can be done?
* What options are available?
* What are the associated trade-offs in terms of costs, benefits, and risks?
* What are the impacts of current management decisions (i.e., policy) on future options?

Answering the last question leads to the optimal solution. Thus, risk management is a systematic, statistically-based, holistic process that employs formal risk assessment and management techniques to address the sources of system failures. This approach can help security managers provide the right information to senior managers to help them make informed decisions.

**In what 3 general ways can risk be reduced? Prevent, Detect, Mitigate**

**Design Basis Threat (DBT)**

The **design basis threat** (DBT) is a profile of the type, composition, and capabilities of an adversary. The DBT is a threat estimate that includes intelligence, reports, assessments, statistics, and supporting information.

Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence.

The key distinction between security and safety events is their cause—accidental, unintentional, or natural disaster (abnormal event) versus malevolent, intentional human-caused events.

**What is a design basis threat?**

* ****

**a profile of the type, composition, and capabilities of an adversary.**

* ****

**a threat estimate that includes intelligence, reports, assessments, statistics, and supporting information**

* ****

**a document that requires requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence.**

* ****

**All of the above**

In the DBT context, the threat comes from malevolent humans, not accidental (safety-related) events. While safety and security are related and complementary functions, a physical protection system (PPS) is implemented primarily to stop malevolent attacks, not to prevent fires or respond to acts of nature or unintentional human errors.

**A PPS is implemented to primarily address what? Malevolent attacks**

**Which is not a component of a design basis threat? Path Analysis**

**When a lot of data is available, what is typically the best way to calculate the likelihood of attack?**

**Frequency**

**Costs to Be Considered**

Costs of security losses are both direct and indirect.

* Direct costs include the loss of money, negotiable instruments, property, or information.
* Indirect costs include harm to reputation, loss of goodwill, loss of employees, and harm to employee morale.

Both direct and indirect costs can be measured in terms of lost assets and lost income. Often, a single loss results in both kinds of costs.

The use of money for loss replacement represents an additional cost margin and is called **lost income**. One formula is as follows:

I = (i/365) x P x T

I = income earned  
i = annual percent rate of return  
P = principal amount (in dollars) available for investment  
T = time (in days) during which P is available for investment

For example, the income earned from $1,000, invested at 10 percent per annum for a period of 90 days, would be $24.66.

**Which is least likely to be a component of the cost of a temporary substitute for a lost asset?**

**Depreciation**

**(i/365) x P x T is the formula for what? Lost income cost**

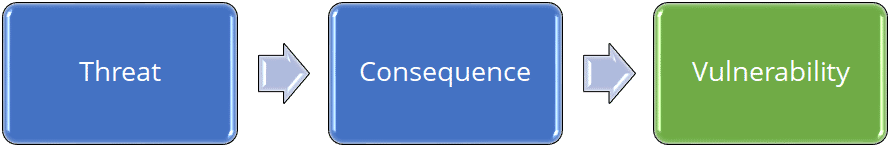
**Cost-of-Loss Formula**

Taking the worst-case position and analyzing each security vulnerability for the probable maximum loss for a single occurrence of the risk event, one can use the following equation:

**K = (Cp + Ct + Cr + Ci) - (I - a)**

K = criticality, total cost of loss  
Cp = cost of permanent replacement  
Ct = cost of temporary substitute  
Crm = total related costs  
Ci = lost income cost  
I = available insurance or indemnity  
a = allocable insurance premium amount

**Which is most likely to be used as a measure for loss of reputation? Loss of sales**



**Vulnerability Assessment**

A **vulnerability** is a weakness that can be exploited by an adversary. **Vulnerability assessment** or analysis (VA) is the process of identifying and quantifying the weak points of a facility, entity, venue, or person.

A VA must be performed once to establish the baseline of protection system effectiveness; it may be repeated to verify the effectiveness of a proposed upgrade, and then conducted again periodically to verify that the system is performing as required. The VA may provide different results against different threats, as each element of the Physical Protection System (PPS) performs differently against different threats.

**Vulnerability Assessment Objectives**

* Facility characterization
* Evaluation of the facility’s PPS
* A site survey of detection, delay, and response (Five D) components
* Data to estimate their performance against particular threats

**Who should lead the vulnerability assessment team? A Security Specialist**

*The key to the vulnerability assessment  is to thoroughly evaluate the system so that all paths to the assets are equally protected, and to consider what vulnerabilities exist given the defined threats.*

What is the biggest mistake when conducting a vulnerability assessment? Not considering the PPS at

the system level

The VA team needs to determine whether the physical protection system is more or less vulnerable during different facility states (24/7/365). Examples of facility states include normal operating hours, nonoperational hours, a strike at the facility, emergencies (e.g., fires or bomb threats), varying weather conditions, and shift changes.

**00:58**

**How should a vulnerability assessment report be prepared? In the manner most useful to the facility**

**What are the three dimensions of management? Technical expertise, management ability, ability to**

**deal with people.**

**Where should security be placed in the corporate structure? Placed as high as possible in the**

**structure of an enterprise and report directly to senior or executive mgmt.**

**Whose customers might include investors, clients, and self? Independent consultants**

Unity of command dictates that an individual report to only one supervisor.

Lines of authority responsibilities and comm should be as clear and direct as possible

Span of control suggests that a single person can supervise only a limited # of staff effectively

**It becomes apparent that a guard supervisor responsible for 20 officers can't effectively manage all of them. This demonstrates which concept? Span of control**

The most famous management systems standards (used by more than a million organizations in 161 countries) are the **ISO quality management systems standard** and **environmental management systems standard**.

*Management systems standards* ***provide a framework for what an organization should do*** *while leaving '****how to do it' to the discretion of the organization*** *based on its financial and operating environment.*

**Which statement is true about management systems? They provide the framework for what to do not how to do it.**

**What organization published "Security and Resilience in Organizations and their Supply Chains—Requirements with Guidance (ORMS)"? ASIS**

***Security and Resilience in Organizations and their Supply Chains—Requirements with Guidance (ASIS ORM.1-2017)***. The **ORMS** management system standard provides an integrated, risk-based management systems approach to manage risk and enhance resilience in organizations and their supply chains.

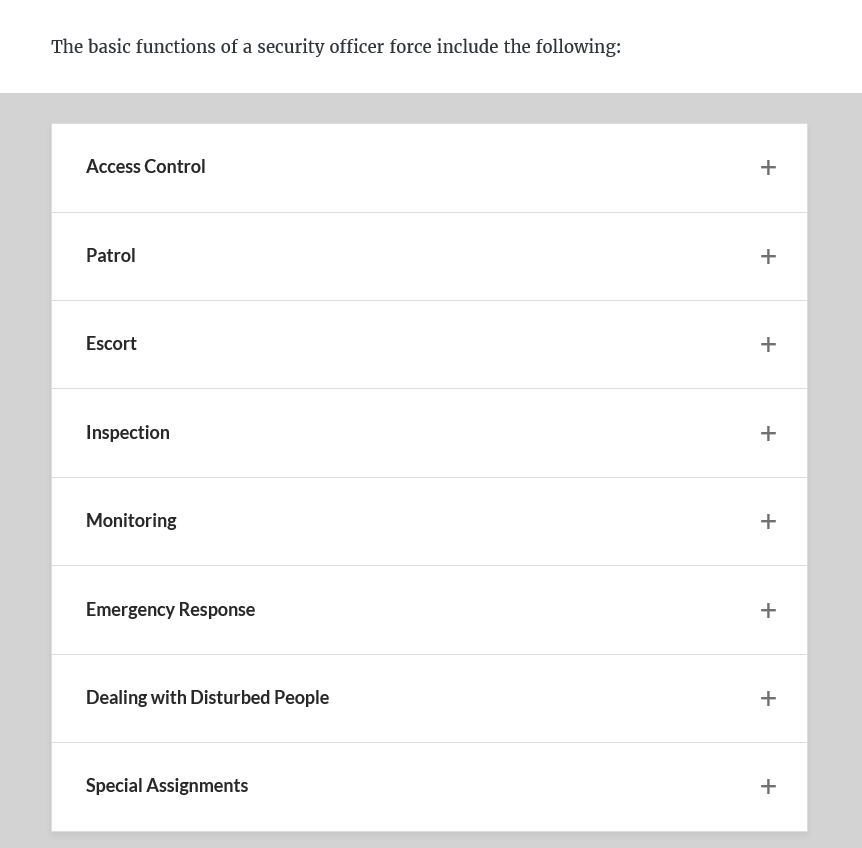
*The Plan-Do-Check-Act  (PDCA) or Deming continuous improvement model*

Establish management system policy, objectives, processes, and procedures relevant to managing operations and improving risk management to deliver results in accordance with an organization’s overall policies and objectives.The PDCA model is a clear, systematic, and documented approach to:

* Set measurable objectives and targets
* Monitor, measure, and evaluate progress
* Identify, prevent or remedy problems as they occur
* Assess competency requirements and train persons working on the organization's behalf
* Provide top management with a feedback loop to assess progress and make appropriate changes to the management system.

**Which model does the ORMS standard use to structure the security and resilience processes?**

**Plan-Do-Check-Act**

**BASIC FUNCTIONS flashcard**

**Which is not normally considered a special assignment for a security officer? Dealing with disturbed**

**persons**

The decision on whether to arm an officer should be based on the existence of one or both of the following conditions:

* There is a greater danger to life safety without the weapon.
* The officer may reasonably be expected to use fatal force.

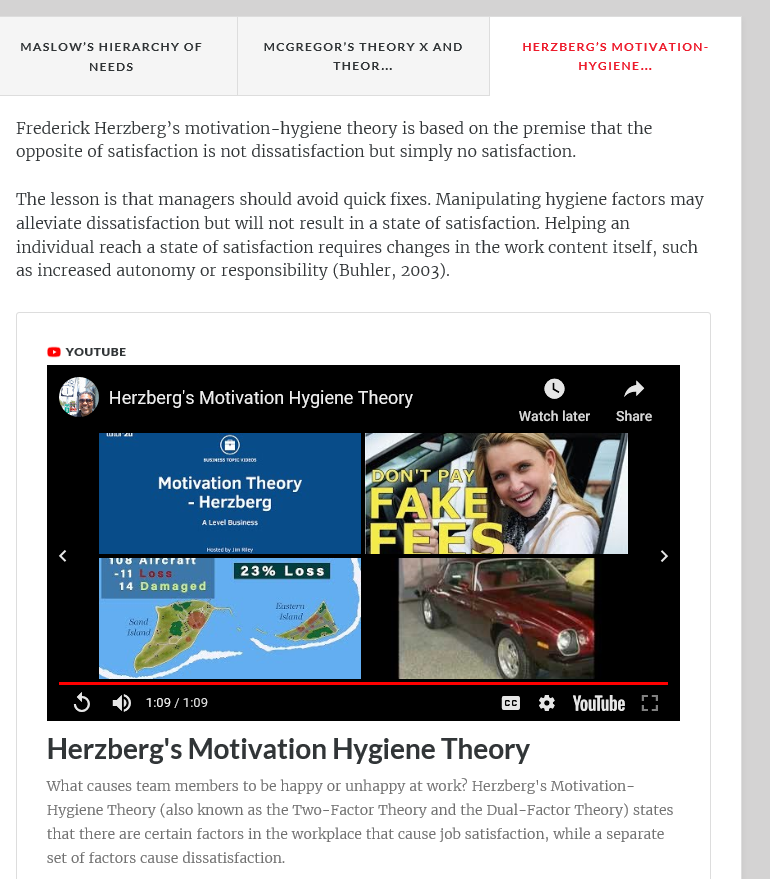
The real test would be whether the actual losses were less than the probable losses and whether the combined cost of the actual losses and the cost of maintaining the asset protection organization were within the risk-assumption boundaries accepted by management when approving the asset protection program.

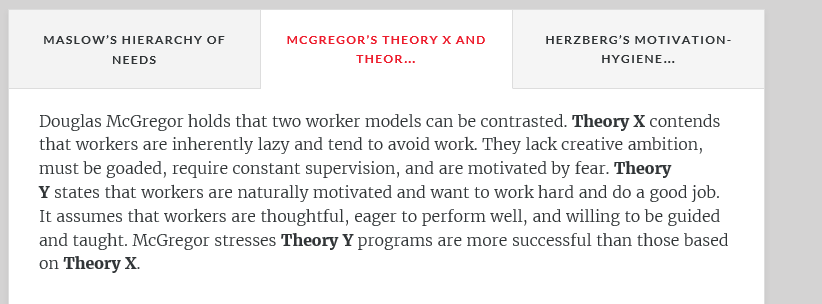
**In which security-structure model are employees are connected just to their immediate supervisor and to those whom they themselves supervise, but also to many others in the organization? Network**

**Which is typically not a major issue when considering whether to use contract officers or proprietary officers? The strategic security plan**

**Private police may lack the moral authority that government can confer upon law enforcement. This is**

**Which item is at the midpoint of Maslow's Hierarchy of Needs? Security**





**Workers are naturally motivated and want to work hard and do a good job. It assumes that workers are thoughtful, eager to perform well, and willing to be guided and taught. This theory is known as what?**

**Theory Y**

**In which situation would behavioral science methods be least useful? Vendor selection**